IX. CLAIMS

I claim:

1. A method of encrypting and decrypting information, comprising:
   (a) providing information and a key,
   (b) using said key to help construct a state generator and a sequence of permutations,
   (c) constructing a sequence of states with said state generator, and permuting said information with said sequence of permutations,
   (d) encrypting said information with said sequence of states if the permuted information is a message and decrypting said information with said sequence of states if the permuted information is ciphertext.

2. The method of claim 1 wherein a perturbator changes a permutation to help generate said sequence of permutations.

3. The method of claim 1 wherein said method is used in a consumer product.

4. The method of claim 1 wherein said method is used in a wireless application.

5. The method of claim 1 wherein in (d) encrypting and decrypting use one of the following functions: an exclusive-or function, an addition modulo L function, a subtraction modulo L function, or a permutation function.

6. The method of claim 1 wherein said state generator is a dynamical system.

7. The method of claim 6 wherein said dynamical system is iterative.

8. The method of claim 6 wherein said dynamical system is non-iterative.

9. The method of claim 6 wherein said dynamical system is non-autonomous.

10. The method of claim 6 wherein a matrix is used to generate said dynamical system.

11. The method of claim 10 wherein said matrix is changed with a

perturbator.

12. The method of claim 11 wherein said perturbator uses a zero repeller.

13. The method of claim 6 wherein one or more permutations are used to generate said dynamical system.

14. The method of claim 13 wherein said permutations, that generate said dynamical system, create said sequence of states.

15. The method of claim 13 wherein said permutations are changed with a perturbator.

16. The method of claim 6 wherein said dynamical system is changed with a perturbator.

17. The method of claim 16 wherein said perturbator is implemented with a dynamical system.

18. A method of encrypting and decrypting information, comprising:

(a) providing information and a key,

(b) using said key to help construct a state generator and a sequence of permutations,

(c) constructing a sequence of states with said state generator,

(d) permuting said sequence of states with said sequence of permutations,

(e) encrypting said information with the permuted sequence of states if said information is a message and decrypting said information with the permuted sequence of states if said information is ciphertext.

19. The method of claim 18 wherein a perturbator changes a permutation to help generate said sequence of permutations.

20. The method of claim 18 wherein said method is used in a consumer product.

21. The method of claim 18 wherein said method is used in a wireless application.

22. The method of claim 18 wherein in (e) encrypting and decrypting use

one of the following functions: an exclusive-or function, an addition modulo L function, a subtraction modulo L function, or a permutation function.

23. The method of claim 18 wherein said state generator is a dynamical system.

24. The method of claim 23 wherein said dynamical system is iterative.

25. The method of claim 23 wherein said dynamical system is non-iterative.

26. The method of claim 23 wherein said dynamical system is non-autonomous.

27. The method of claim 23 wherein a matrix is used to generate said dynamical system.

28. The method of claim 27 wherein said matrix is changed with a perturbator.

29. The method of claim 28 wherein said perturbator uses a zero repeller.

30. The method of claim 23 wherein one or more permutations are used to generate said dynamical system.

31. The method of claim 30 wherein said permutations, that generate said dynamical system, create said sequence of states.

32. The method of claim 30 wherein said permutations are changed with a perturbator.

33. The method of claim 23 wherein said dynamical system is changed with a perturbator.

34. The method of claim 33 wherein said perturbator is implemented with a dynamical system.

35. A cryptographic machine, comprising:

(a) information,

(b) a sequence of permutations, which permutes said information,

(c) a state generator, which constructs a sequence of states,

(d) a key, which determines said sequence of permutations and said state generator.

whereby if the permuted information is a permuted message, then said sequence of states encrypts said permuted message and if the permuted information is permuted ciphertext then said sequence of states decrypts said permuted ciphertext.

36. The machine of claim 35 wherein a perturbator changes a permutation to help generate said sequence of permutations.

37. The machine of claim 35 wherein said machine runs in a consumer product.

38. The machine of claim 35 wherein said machine runs in a wireless application.

39. The machine of claim 35 wherein the encryption and decryption use one of the following functions: an exclusive-or function, an addition modulo L function, a subtraction modulo L function, or a permutation function.

40. The machine of claim 35 wherein said state generator is a dynamical system.

41. The machine of claim 40 wherein said dynamical system is iterative.

42. The machine of claim 40 wherein said dynamical system is non-iterative.

43. The machine of claim 40 wherein said dynamical system is non-autonomous.

44. The machine of claim 40 wherein a matrix is used to generate said dynamical system.

45. The machine of claim 44 wherein said matrix is changed with a perturbator.

46. The machine of claim 45 wherein said perturbator uses a zero repeller.

47. The machine of claim 40 wherein one or more permutations are used to generate said dynamical system.

48. The machine of claim 47 wherein said permutations, that generate said dynamical system, create said sequence of states.

49. The machine of claim 47 wherein said permutations are changed with a perturbator.

50. The machine of claim 40 wherein said dynamical system is changed with a perturbator.

51. The machine of claim 50 wherein said perturbator is implemented with a dynamical system.

52. A cryptography machine, comprising:

(a) information

(b) a state generator, which constructs a sequence of states,

(c) a sequence of permutations, which permutes said sequence of states,

(d) a key, which determines said state generator and said sequence of permutations,

whereby if said information is a message, then the permuted sequence of states encrypts said message and if said information is ciphertext then the permuted sequence of states decrypts said ciphertext.

53. The machine of claim 52 wherein a perturbator changes a permutation to help generate said sequence of permutations.

54. The machine of claim 52 wherein said machine runs in a consumer product.

55. The machine of claim 52 wherein said machine runs in a wireless application.

56. The machine of claim 52 wherein the encryption and decryption use one of the following functions: an exclusive-or function, an addition modulo L function, a subtraction modulo L function, or a permutation function.

57. The machine of claim 52 wherein said state generator is a dynamical system.

58. The machine of claim 57 wherein said dynamical system is iterative.

59. The machine of claim 57 wherein said dynamical system is non-iterative.

60. The machine of claim 57 wherein said dynamical system is non-autonomous.

61. The machine of claim 57 wherein a matrix is used to generate said dynamical system.

62. The machine of claim 61 wherein said matrix is changed with a perturbator.

63. The machine of claim 62 wherein said perturbator uses a zero repeller.

64. The machine of claim 57 wherein one or more permutations are used to generate said dynamical system.

65. The machine of claim 64 wherein said permutations, that generate said dynamical system, create said sequence of states.

66. The machine of claim 64 wherein said permutations are changed with a perturbator.

67. The machine of claim 57 wherein said dynamical system is changed with a perturbator.

68. The machine of claim 67 wherein said perturbator is implemented with a dynamical system.

69. A cryptographic machine, comprising:

(a) information

(b) one or more non-autonomous dynamical systems, which generate a sequence of states,

(c) a key which determines each said non-autonomous dynamical system

whereby if said information is a message, then said machine encrypts said message using the states of one or more of said non-autonomous dynamical systems and if said information is ciphertext, then machine decrypts said ciphertext using the states of one or more of said non-autonomous dynamical systems.

70. The machine of claim 69 wherein each said non-autonomous dynamical system is implemented with a distinct sequence of permutations.

71. The machine of claim 69 wherein each said sequence of permutations is implemented using a perturbator.

72. The machine of claim 69 wherein said method is used in a consumer product.

73. A method of encrypting and decrypting information, comprising:

(a) providing information and a key,

(b) using said key to help construct a sequence of permutations,

(c) encrypting said information with said sequence of permutations if said information is a message and decrypting said information with said sequence of permutations if said information is ciphertext.

74. The method of claim 73 wherein a perturbator changes a permutation to help generate said sequence of permutations.

75. The method of claim 73 wherein said method is used in a wireless application.

76. The method of claim 73 wherein said method is used in a consumer product.

77. A method of generating random numbers, comprising:

(a) providing a state generator and sequence of permutations,

(b) generating a sequence of states with said state generator,

(c) permuting sequence of states with said sequence of permutations,

(d) extracting random numbers from the permuted sequence of states.

78. The method of claim 77 wherein said random numbers are used as encryption and decryption keys.

X. REFERENCES

[FISKE] Michael Fiske. (1996)
Non-autonomous dynamical systems applied to neural computation.
Ph.D. Thesis, Northwestern University.

[NYTIMES] Markoff, John. (July 17, 1998)
U.S. Data-Scrambling Code Cracked With Homemade Equipment.
New York Times.

[ROBINSON] Robinson, Clark. (1995)
Dynamical Systems Stability, Symbolic Dynamics, and Chaos.
CRC Press.

[SCHNEIER] Schneier, Bruce. (1996)
APPLIED CRYPTOGRAPHY.
John Wiley & Sons, Inc.

[SPIVAK] Spivak, Mike. (1979)
DIFFERENTIAL GEOMETRY. Volume I.
Publish or Perish, Inc.